House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 234* **House Bill No. 528**

by deleting all language after the enacting clause and substituting:

SECTION 1. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-5601.

As used in this part:

(1) "Affiliate" means any person controlling, controlled by, or under common control with such person;

(2) "Division" means the division of consumer affairs in the office of the attorney general and reporter; and

(3) "Person" means a natural person, individual, governmental agency, partnership, corporation, trust, estate, incorporated or unincorporated association, and any other legal or commercial entity however organized, including any affiliate.

47-18-5602.

(a)

(1) A person shall not contact a property owner more than one (1) time in a calendar year in connection with an unsolicited request to buy the property owner's real property.

(2) The limitation described in subdivision (a)(1) applies to contact made through a telephone call, text message, email, mail, facsimile transmission, or another form of contact.

(b) When a person contacts a property owner in connection with an unsolicited request to buy the property owner's real property, prior to making the solicitation, the person shall provide to the property owner:

(1) The person's legal name;

(2) The address from which the person operates;

(3) A telephone number at which the person can be contacted; and

(4) An email address at which the person can be contacted.

47-18-5603.

(a) If a property owner believes a person has violated § 47-18-5602, then the property owner may submit a complaint to the division. The division shall:

(1) Begin reviewing a complaint submitted pursuant to this subsection (a) within twenty (20) business days from the date the complaint is submitted;

(2) Send a written notice to the property owner that the division is reviewing the complaint; and

(3) Send a written notice to the property owner upon completion of the review describing the findings of the review, including whether the individual who contacted the property owner is a licensed real estate agent, and the actions taken, if any, as a result of the findings.

(b)

(1) With regard to alleged violations of this part, the attorney general and reporter has all of the investigative and enforcement authority that the attorney general and reporter has under part 1 of this chapter. The attorney general and reporter may institute a proceeding involving alleged violations of this part in Davidson County circuit or chancery court or another venue otherwise permitted by law.

(2) The attorney general and reporter shall require the person being investigated pursuant to a complaint submitted in accordance with subsection (a)

to disclose any affiliates of the person that have sent an unsolicited request to buy the property owner's real property.

(3) If a court finds that a person violated § 47-18-5602, then the court shall assess a fine of up to one thousand five hundred dollars ($1,500) per violation. The court may also order reimbursement to this state for the reasonable costs and expenses of investigation and prosecution of actions under this part, including attorneys' fees.

(4) For purposes of determining how many violations a person has committed, each contact beyond the permitted number under § 47-18-5602 by a person, including any affiliate of the person, is a separate violation.

47-18-5604.

This part does not apply to an individual who is licensed as a real estate agent in the state in which the real property about which the individual contacted the property owner is located.

SECTION 2. This act takes effect July 1, 2023, the public welfare requiring it, and applies to prohibited conduct occurring on or after that date.

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 1285 **House Bill No. 1060***

by deleting all language after the enacting clause and substituting:

SECTION 1. Tennessee Code Annotated, Section 50-7-302(a), is amended by deleting subdivision (4) and substituting:

(4)

(A) The claimant is able to work, available for work, and making a reasonable effort to secure work. As used in this subdivision (a)(4)(A), "making a reasonable effort to secure work" means the claimant provides detailed information regarding at least five (5) work search activities per week;

(B) The following actions are acceptable work search activities that count toward the requirement of subdivision (a)(4)(A) that a claimant is making a reasonable effort to secure work:

(i) A department-approved job search or skills assessment;

(ii) Completion of a department-approved job search plan;

(iii) Participating in an on-the-job training opportunity;

(iv) Taking a civil service exam;

(v) Developing a complete resume in the state's employment service system;

(vi) Submitting a resume to an employer;

(vii) Completing and submitting a job application to an employer;

(viii) Attending and completing an interview with an employer;

(ix) Attending a job fair; or

(x) Completing a skills test assigned by an employer as part of an interview process;

(C)

(i) The administrator shall:

(a) Verify whether claimants are complying with the requirement of at least five (5) work search activities per week; and

(b) Disqualify any claimant receiving benefits who the administrator finds has provided false work search information;

(ii) In determining whether the claimant is making a reasonable effort to secure work, the administrator shall consider the customary methods of obtaining work in the claimant's usual occupation or occupation for which the claimant is reasonably qualified, the current condition of the labor market, and any attachment the claimant may have to a regular job;

(D) A claimant shall not be considered ineligible in any week of unemployment for failure to comply with this subsection (a) if the failure is due to an illness or disability that occurred after the claimant has registered for work, and no work that would have been considered suitable at the time of the claimant's initial registration has been offered after the beginning of the illness or disability. The administrator may, however, in the administrator's discretion, require the claimant to obtain and submit a certificate by a duly licensed physician as to the illness or disability with respect to each week that the illness or disability exists;

(E) An otherwise eligible claimant shall not be denied benefits for any week because the claimant is in training with the approval of the administrator, nor shall the claimant be denied benefits with respect to any week in which the

claimant is in training with the approval of the administrator by reason of the application of this subsection (a) relating to availability for work, or of § 50-7-303(a)(3) relating to failure to apply for, or refusal to accept, suitable work;

(F) The unemployment of a claimant for any week or any portion of a week, caused by a plant, departmental, or other type of shutdown for vacation purposes, must not be the basis for a denial of benefits for the week, or portion of a week, if the claimant has not or will not receive any vacation pay from the claimant's employer for the period, when so found by the administrator;

(G) An otherwise eligible claimant shall not be denied benefits by reason of the application of this subsection (a) who, subsequent to the claimant's enrollment in and while attending a regularly established school, college, or university, has been regularly employed and becomes unemployed and makes the claimant available for all suitable work, as determined by the administrator, to the same extent that the claimant was previously employed while continuing to attend and be enrolled in the regularly established school, college, or university; provided, that if the claimant is offered the same job that the claimant previously held immediately prior to entering the school and refuses the job, then the claimant is ineligible for the benefits provided by this chapter if the job meets the standards set forth in § 50-7-303(a)(3)(A) and (B) as required by applicable federal law;

(H) This subsection (a) or any other provision of law must not be construed to deny unemployment benefits to any claimant who is a veteran enrolled in school under the Veterans' Educational Assistance Program, commonly known as the "G.I. Bill" (38 U.S.C. § 1650 et seq.), solely because of the claimant's enrollment and attendance in school, if the claimant is otherwise eligible for the benefits, except that if the claimant is offered the same job that the claimant previously held immediately prior to entering the school and refuses the

job, then the claimant shall become ineligible for benefits as provided by § 50-7-303(a)(3) if the job meets the standards set forth in § 50-7-303(a)(3)(A) and (B) as required by applicable federal law; and

(I) A claimant is ineligible for benefits if the claimant is incarcerated four (4) or more days in any week for which unemployment benefits are being claimed;

SECTION 2. Tennessee Code Annotated, Section 50-7-303(a)(3), is amended by adding the following as a new subdivision:

(C)

(i) A claimant who fails to appear for a scheduled job interview is non-compliant with the work search requirements of the unemployment insurance program. A claimant is disqualified for the week the failure occurred;

(ii)

(a) The department shall establish a portal on its website, and an email and telephone hotline, for employers to report an unemployment insurance claimant who fails to appear for a scheduled job interview;

(b) The department shall:

(1) Establish a portal on its website, and an email and telephone hotline, for employers to report an unemployment insurance claimant who fails to appear for a scheduled job interview; and

(2) Communicate annually with employers in this state that participate in the unemployment insurance program of the employer's right to use the portal to report suspected unemployment insurance program violations;

SECTION 3. This act takes effect July 1, 2024, the public welfare requiring it.

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 649 **House Bill No. 650***

by deleting all language after the enacting clause and substituting:

SECTION 1. This act is known and may be cited as the "Booting Consumer Protection Act."

SECTION 2. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-3201.

As used in this part:

(1) "Authorized vehicle immobilization device operator" or "operator" means a person authorized by a political subdivision of this state to be engaged in the business of installing vehicle immobilization devices within the jurisdictional area of the political subdivision;

(2) "Engaged in the business of installing vehicle immobilization devices" means installing or removing vehicle immobilization devices on motor vehicles in exchange for monetary payment or other valuable consideration, whether such payment or consideration is received for the installation or the removal of the vehicle immobilization device;

(3) "Person" means an individual, sole proprietor, independent contractor, partnership, corporation, or similar business entity;

(4) "Political subdivision" means a municipality, public corporation, body politic, authority, district, metropolitan government, county, or an agency, department, or board of such entities; and

(5) "Vehicle immobilization device" means a mechanical device that is designed or adapted to be attached to a wheel, tire, or other part of a parked motor vehicle to prohibit the motor vehicle's usual manner of movement or operation.

47-18-3202.

(a) A person engaged in the business of installing vehicle immobilization devices on motor vehicles in this state shall:

(1) Accept credit cards and debit cards as methods of payment for the removal of a vehicle immobilization device from a motor vehicle; and

(2) If the person who is requesting removal of the vehicle immobilization device elects to make the payment by credit card or debit card and the payment cannot be completed by the card without undue delay at the site where the motor vehicle to which the vehicle immobilization device is attached is located, and an optional online payment method as described in subdivision (c)(3) is either unavailable or has been refused by the individual, remove the vehicle immobilization device and issue a billing invoice for payment due:

(A) To the individual who is requesting the removal of the vehicle immobilization device, if such individual provides a valid form of identification; or

(B) By mail to the registered owner of the vehicle.

(b)

(1) A person engaged in the business of installing vehicle immobilization devices on motor vehicles shall utilize for the work of installing and removing such devices only those persons who are required to file a W-2 wage and tax statement with the federal internal revenue service for the compensation those persons receive for the work performed.

(2) A person engaged in the business of installing vehicle immobilization devices on motor vehicles shall not:

(A) Contract for or engage the services of an independent contractor to install or remove vehicle immobilization devices; or

(B) Compensate employees on a commission basis.

(c)

(1) Subsection (a) does not prohibit a person engaged in the business of installing vehicle immobilization devices on motor vehicles from accepting cash or other methods of payment if the person making such payment, in that person's sole discretion, elects to use such alternative payment method.

(2) A person engaged in the business of installing vehicle immobilization devices on motor vehicles shall not charge a fee to accept payment by credit card or debit card.

(3) A person engaged in the business of installing vehicle immobilization devices on motor vehicles may offer an alternative, online payment service as an optional payment method. If the person making payment for the removal of the vehicle immobilization device elects, in the person's sole discretion, to use the optional online payment method, then the provider of the online payment service may charge a three percent (3%) convenience fee. This subdivision (c)(3) supersedes all local ordinances, rules, or other enactments to the contrary.

(4)

(A) If a vehicle immobilization device is placed on a vehicle that is parked on private property due to the vehicle owner's failure to pay the required parking charge, then the owner or operator of the private property may require the owner of the vehicle to pay the applicable immobilization device removal fee and all unpaid parking fines and fees to have the immobilization device removed.

(B) This subdivision (c)(4) supersedes all local ordinances, rules, or other enactments to the contrary.

(d)

(1)

(A) An owner, lessee, or other person who has control of a property for which an enforceable agreement exists with a person engaged in the business of installing vehicle immobilization devices to provide parking enforcement services by installing vehicle immobilization devices on motor vehicles on such property shall post signage in a conspicuous location on the property bearing notice:

(i) That the parking policy for the property is strictly enforced;

(ii) That a violator's vehicle will be immobilized with a vehicle immobilization device with the owner of the vehicle having to pay to have the device removed;

(iii) Of the name and phone number of the authorized vehicle immobilization device operator; and

(iv) That consumers are protected from violations of this part and that violations may be reported to the attorney general and reporter.

(B) The sign required by this subdivision (d)(1) must:

(i) Be no less than twenty-four inches (24") in height and eighteen inches (18") in width and contain lettering that is no less than two inches (2") in height; and

(ii)

(*a*) Be located at each designated entrance to the property where parking prohibitions are in place; or

(*b*) If there is no designated entrance, be erected in a place that is clearly visible from each parking space.

(C) Notwithstanding subdivisions (d)(1)(A) and (B)(i), if on the effective date of this act a property has existing signage posted that contains the notice required by subdivisions (d)(1)(A)(i)-(iii), then the signage complies with subdivision (d)(1)(A) and is exempt from the requirements of subdivision (d)(1)(B)(i) if the notice required by subdivision (d)(1)(A)(iv) is permanently affixed adjacent to the existing signage. However, new or replacement signage installed on or after the effective date of this act must comply with subdivisions (d)(1)(A) and (B)(i).

(2) A person engaged in the business of installing vehicle immobilization devices shall not install a vehicle immobilization device on a motor vehicle if the motor vehicle is located on property that does not comply with the signage requirements under subdivision (d)(1).

47-18-3203.

(a) A violation of this part constitutes a violation of the Tennessee Consumer Protection Act of 1977.

(b) A violation of this part constitutes an unfair or deceptive act or practice affecting trade or commerce and is subject to the penalties and remedies as provided in the Tennessee Consumer Protection Act of 1977, in addition to any penalties and remedies established under this part.

(c) If the attorney general and reporter reasonably believes that any person has violated this part, then the attorney general and reporter may institute a proceeding under this chapter.

47-18-3204.

(a) If an authorized vehicle immobilization device operator is found to have violated § 47-18-3202 as part of a final judgment and the operator has no opportunity to appeal the judgment, then the attorney general and reporter shall send notice of the violation to each political subdivision that has authorized the operator to operate within its jurisdictional area.

(b) Upon the receipt of notice from the attorney general and reporter that an operator has committed a third violation of § 47-18-3202, a political subdivision shall permanently revoke the operator's authorization to engage in the business of installing vehicle immobilization devices within the jurisdictional area of the political subdivision.

SECTION 3. Tennessee Code Annotated, Section 47-18-104(b), is amended by adding the following as a new subdivision:

( ) Violating § 47-18-3202.

SECTION 4. This act takes effect July 1, 2023, the public welfare requiring it, and applies to prohibited conduct occurring on or after that date.

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 1295 House Bill No. 1310*

by deleting all language after the enacting clause and substituting:

SECTION 1. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-4901.

This part is known as the "Genetic Information Privacy Act."

47-18-4902.

As used in this part:

(1) "Biological sample" means a human material known to contain DNA, including tissue, blood, urine, or saliva;

(2) "Consumer" means an individual who is a resident of the state;

(3) "Deidentified data" means data that:

(A)

(i) Cannot reasonably be linked to an identifiable individual; or

(ii) Meets the standard for deidentification under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. § 1320d et seq.) and rules promulgated pursuant to that act; and

(B) Is possessed by a company that:

(i) Takes administrative and technical measures to ensure that the data cannot be associated with a particular consumer;

(ii) Makes a public commitment to maintain and use data in deidentified form and not attempt to reidentify data; and

(iii) Enters into a legally enforceable contractual obligation that prohibits a recipient of the data from attempting to reidentify the data;

(4) "Direct-to-consumer genetic testing company" or "company":

(A) Means an entity that:

(i) Offers consumer genetic testing products or services directly to a consumer; or

(ii) Collects, uses, or analyzes genetic data that resulted from a direct-to-consumer genetic testing product or service and was provided to the company by a consumer; and

(B) Does not include:

(i) A law enforcement agency; or

(ii) An entity that is, and only while, engaged in collecting, using, or analyzing genetic data or biological samples in the context of research, as defined in 45 CFR § 164.501, that is conducted in accordance with:

(*a*) The Federal Policy for the Protection of Human Subjects, as described in 45 CFR Part 46;

(*b*) The Good Clinical Practice Guideline issued by the International Council for Harmonization; or

(*c*) The United States Food and Drug Administration Policy for the Protection of Human Subjects under 21 CFR Parts 50 and 56;

(5) "DNA" means deoxyribonucleic acid;

(6) "Express consent" means a consumer's affirmative response to a clear, meaningful, and prominent notice regarding the collection, use, or disclosure of genetic data for a specific purpose;

(7) "First-party relationship" means the relationship between a company and a consumer from which the company has collected genetic data;

(8) "Genetic data" means data, excluding deidentified data, regardless of format, concerning a consumer's genetic characteristics, including:

(A) Raw sequence data that results from sequencing all or a portion of a consumer's extracted DNA;

(B) Genotypic and phenotypic information obtained from analyzing a consumer's raw sequence data; or

(C) Self-reported health information regarding a consumer's health conditions that the consumer provides to a company and that the company:

(i) Uses for scientific research or product development; and

(ii) Analyzes in connection with the consumer's raw sequence data;

(9) "Genetic testing" means:

(A) A laboratory test of a consumer's complete DNA, regions of DNA, chromosomes, genes, or gene products to determine the presence of genetic characteristics of the consumer; or

(B) An interpretation of a consumer's genetic data; and

(10) "Person" means an individual, corporation, business, partnership, limited liability company, or other business entity.

47-18-4903.

This part does not apply to:

(1) Protected health information that is collected by a covered entity or business associate as those terms are defined in 45 CFR Parts 160 and 164;

(2) A public or private institution of higher education;

(3) An entity owned or operated by a public or private institution of higher education;

(4) Biomedical or academic research conducted by a research hospital, academic medical center, or other entity affiliated with such hospital or medical center that is not a direct-to-consumer genetic testing company;

(5) Genetic data that is shared with or by a research hospital, academic medical center, or other entity affiliated with such hospital or medical center that is not a direct-to-consumer genetic testing company for the purposes of biomedical or academic research or to find causes of or cures for a disease or medical condition; or

(6) The sharing of genetic data that does not require consent pursuant to the Federal Policy for the Protection of Human Subjects, as described in 45 CFR Part 46.

47-18-4904.

(a) A direct-to-consumer genetic testing company shall:

(1) Provide to a consumer:

(A) Essential information about the company's collection, use, and disclosure of genetic data; and

(B) A prominent, publicly available privacy notice that includes information about the company's data collection, consent, use, access, disclosure, transfer, security, retention, and deletion practices;

(2) Obtain a consumer's initial express consent for collection, use, or disclosure of the consumer's genetic data that:

(A) Clearly describes the company's use of the genetic data that the company collects through the company's genetic testing product or service;

(B) Specifies who has access to test results; and

(C) Specifies how the company may share the genetic data;

(3) If the company engages in the following conduct, obtain a consumer's:

(A) Separate express consent for:

(i) The transfer or disclosure of the consumer's genetic data to a person other than the company's vendors and service providers;

(ii) The use of genetic data beyond the primary purpose of the company's genetic testing product or service; or

(iii) The company's retention of a biological sample provided by the consumer following the company's completion of the initial testing service requested by the consumer;

(B) Informed consent in accordance with the Federal Policy for the Protection of Human Subjects, as described in 45 CFR Part 46, for transfer or disclosure of the consumer's genetic data to a third party for:

(i) Research purposes; or

(ii) Research conducted under the control of the company for the purpose of publication or generalizable knowledge; and

(C) Express consent for:

(i) Marketing to a consumer based on the consumer's genetic data; or

(ii) Marketing by a third-party person to a consumer based on the consumer having ordered or purchased a genetic testing product or service;

(4) Require valid legal process for the company's disclosure of a consumer's genetic data to law enforcement or a government entity without the consumer's express written consent;

(5) Develop, implement, and maintain a comprehensive security program to protect a consumer's genetic data against unauthorized access, use, or disclosure; and

(6) Provide a process for a consumer to:

(A) Access the consumer's genetic data;

(B) Delete the consumer's account and genetic data; and

(C) Destroy the consumer's biological sample.

(b) Notwithstanding subdivision (a)(3)(C), a direct-to-consumer genetic testing company with a first-party relationship to a consumer may, without obtaining the consumer's express consent, provide customized content or offers on the company's website or through the company's application or service.

47-18-4905.

A direct-to-consumer genetic testing company shall not disclose a consumer's genetic data without first obtaining the consumer's written consent to:

(1) An entity that offers health insurance, life insurance, or long-term care insurance; or

(2) An employer of the consumer.

47-18-4906.

The division of consumer affairs in the office of the attorney general and reporter shall enforce this part. The division shall:

(1) Establish a means by which a consumer can submit a complaint for a violation of this part; and

(2) Promulgate rules to effectuate this part. The rules must be promulgated in accordance with the Uniform Administrative Procedures Act, compiled in title 4, chapter 5.

SECTION 2. This act takes effect July 1, 2023, the public welfare requiring it, and applies to conduct occurring on or after that date.

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

_____

Signature of Sponsor

AMEND Senate Bill No. 1043* **House Bill No. 1231**

by deleting all language after the enacting clause and substituting:

SECTION 1. Tennessee Code Annotated, Title 47, Chapter 50, is amended by adding the following as a new section:

(a) As used in this section:

(1) "Entertainment":

(A) Means a form of diversion, recreation, or show; and

(B) Includes:

(i) Theatrical or operatic performances;

(ii) Concerts;

(iii) Motion pictures;

(iv) Shows or events at fair grounds;

(v) Amusement parks; and

(vi) Athletic games or competition, including football, basketball, baseball, boxing, tennis, hockey, or another sport;

(2) "Place of entertainment":

(A) Means a privately or publicly owned facility for entertainment for which an entry fee is charged; and

(B) Includes a theater, stadium, arena, racetrack, museum, amusement park, or other place where performances, concerts, exhibits, or athletic games or contests are held;

(3) "Resale":

(A) Means a sale of a ticket for entrance to a place of entertainment located within the boundaries of this state, other than a sale by the operator or the operator's agent who is expressly authorized to make first sales of the tickets; and

(B) Includes a sale made in person, or by means of telephone, mail, delivery service, facsimile, internet, email, or other electronic means, where the venue for which the ticket grants admission is located in this state;

(4) "Third-party ticket reseller" means an individual, firm, corporation, or other entity that:

(A) Engages in the business of reselling tickets to a place of entertainment;

(B) Operates an internet website or other electronic service that provides a mechanism for two (2) or more parties to participate in a resale transaction;

(C) Facilitates resale transactions by means of an auction; or

(D) Maintains an office, branch of an office, bureau, agency, or other entity for purposes of engaging in the business of reselling tickets to a place of entertainment; and

(5) "Ticket" means evidence of the right of entry to a place of entertainment located within this state.

(b) A third-party ticket reseller, ticket broker, ticket issuer, and ticket resale website shall disclose the total cost of a ticket, including all ancillary fees and service charges, to be paid in order to complete the purchase of a ticket, prior to the ticket being selected for purchase.

(c) The information required to be disclosed pursuant to subsection (b) must be disclosed in a clear and conspicuous manner and in dollars. If a ticket is sold through a

website, then the information required to be disclosed must be displayed in the ticket listing prior to the ticket being selected for purchase. The information disclosed must not be false or misleading, and must not be presented more prominently, or in the same or larger size font, as the total price.

(d) The price of a ticket sold through a website must not increase after a consumer has selected a ticket for purchase, excluding reasonable fees for delivery of non-electronic tickets based on the delivery method selected by the purchaser prior to payment for the ticket.

SECTION 2. Tennessee Code Annotated, Section 39-14-127(a), is amended by adding the following as a new subdivision:

(9) Uses or displays any combination of text, images, website graphics, website display, or website addresses that are substantially similar to the website of an operator with the intent to mislead a potential purchaser, without written authorization. For purposes of this subdivision (a)(9):

(A) "Operator" means an individual, firm, corporation, or other entity, or an agent of such individual, firm, corporation, or other entity that:

(i) Owns, operates, or controls a place of entertainment or that promotes or produces a performance, concert, exhibit, game, athletic event, or contest; and

(ii) Offers for sale a first sale ticket to the place of entertainment or performance, concert, exhibit, game, athletic event, or contest; and

(B) "Place of entertainment" means an entertainment facility in this state, such as a theater, stadium, museum, arena, amphitheater, racetrack, or other place where performances, concerts, exhibits, games, athletic events, or contests are held.

SECTION 3. Tennessee Code Annotated, Section 47-18-104(b), is amended by deleting subdivision (52) and substituting:

(52)

(A)

(1) Using the trade name or trademark, or a confusingly similar trade name or trademark of any place of entertainment, or the name of any event, person, or entity scheduled to perform at a place of entertainment in the domain of a ticket marketplace URL, without written authorization from the place of entertainment, event, person, or entity scheduled to perform at a place of entertainment to use the trade name, trademark, or name in the domain of the URL prior to the use; or

(2) Using or displaying any combination of text, images, website graphics, website display, or website addresses that are substantially similar to the website of an operator with the intent to mislead a potential purchaser, without written authorization from the operator;

(B) For purposes of subdivision (b)(52)(A):

(i) "Domain" means the portion of text in a URL that is to the left of the top-level domains such as .com, .net, or .org;

(ii) "Operator" means an individual, firm, corporation, or other entity, or an agent of such individual, firm, corporation, or other entity that:

(a) Owns, operates, or controls a place of entertainment or that promotes or produces a performance, concert, exhibit, game, athletic event, or contest; and

(b) Offers for sale a first sale ticket to the place of entertainment or performance, concert, exhibit, game, athletic event, or contest;

(iii) "Place of entertainment" means an entertainment facility in this state, such as a theater, stadium, museum, arena, amphitheater,

racetrack, or other place where performances, concerts, exhibits, games, athletic events, or contests are held;

(iv) "Ticket" means a printed, electronic, or other type of evidence of the right, option, or opportunity to occupy space at, to enter, or to attend a place of entertainment, even if not evidenced by any physical manifestation of the right, option, or opportunity; and

(v) "Ticket marketplace" means a website that provides a forum for or facilitates the buying and selling, or reselling, of a ticket;

SECTION 4. Tennessee Code Annotated, Section 47-25-512, is amended by deleting "shall be liable in a civil action by the registrant for any and all of the remedies provided in § 47-25-514, except that under subdivision (2) the registrant shall not be entitled to recover profits or damages unless the acts have been committed with the intent to cause confusion, mistake or deception."; by deleting "any person who:" and substituting "any person who does the following is liable in a civil action by the registrant for any and all of the remedies provided in § 47-25-514, except that under subdivision (2), the registrant is not entitled to recover profits or damages unless the acts have been committed with the intent to cause confusion, mistake, or deception:"; and adding the following as a new subdivision:

(5) Uses or displays any combination of text, images, website graphics, website display, or website addresses that are substantially similar to the website of an operator with the intent to mislead a potential purchaser, without written authorization. For purposes of this subdivision (5):

(A) "Operator" means an individual, firm, corporation, or other entity, or an agent of such individual, firm, corporation, or other entity that:

(i) Owns, operates, or controls a place of entertainment or that promotes or produces a performance, concert, exhibit, game, athletic event, or contest; and

(ii) Offers for sale a first sale ticket to the place of entertainment or performance, concert, exhibit, game, athletic event, or contest; and

(B) "Place of entertainment" means an entertainment facility in this state, such as a theater, stadium, museum, arena, amphitheater, racetrack, or other place where performances, concerts, exhibits, games, athletic events, or contests are held.

SECTION 5. This act takes effect July 1, 2023, the public welfare requiring it, and applies to sales occurring on or after that date.

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

_____

Signature of Sponsor

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____
_____

AMEND Senate Bill No. 996 **House Bill No. 846***

by deleting all language after the enacting clause and substituting:

SECTION 1. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new section:

47-18-135.

(a) As used in this section, "online payment system":

(1) Means an online or mobile system that facilitates the exchange of currency through the internet, including a money transfer or payment; and

(2) Does not include an online or mobile system provided by:

(A) A state or national bank;

(B) A state or federal savings and loan association; or

(C) A state or federal credit union.

(b) An operator of an online payment system shall not freeze the funds of a user without first providing the user with a ninety-day written notice of the online payment system's intent to freeze the user's funds.

(c) The notice requirement of subsection (b) does not apply if an operator of an online payment system has a reasonable belief that financial exploitation, as defined in § 45-2-1202, may have occurred, may have been attempted, or is being attempted, or that a violation of another law has occurred, is occurring, or may occur.

(d) A violation of this section by an online payment system constitutes an unfair or deceptive act prohibited under § 47-18-104, and is punishable as provided in this part.

SECTION 2. Tennessee Code Annotated, Section 47-18-104(b), is amended by adding the following as a new subdivision:

( ) A violation of § 47-18-135;

SECTION 3. This act takes effect July 1, 2023, the public welfare requiring it, and applies to contracts or agreements entered into, amended, or renewed on or after that date.

House Banking & Consumer Affairs Subcommittee Am. #2

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 1285 House Bill No. 1060*

by deleting the amendatory language of SECTION 2 and substituting:

(C)

(i) A claimant who fails to appear for a scheduled job interview is non-compliant with the work search requirements of the unemployment insurance program. A claimant is disqualified for the week the failure occurred;

(ii) The department shall:

(a) Establish a portal on its website, and an email and telephone hotline, for employers to report an unemployment insurance claimant who fails to appear for a scheduled job interview; and

(b) Communicate annually with employers in this state that participate in the unemployment insurance program of the employers' right to use the portal to report suspected unemployment insurance program violations;

House Banking & Consumer Affairs Subcommittee Am. #1

Amendment No._____

FILED
Date _____
Time _____
Clerk _____
Comm. Amdt. _____

Signature of Sponsor

AMEND Senate Bill No. 73* **House Bill No. 1181**

by deleting all language after the enacting clause and substituting:

SECTION 1. This act is known and may be cited as the "Tennessee Information Protection Act."

SECTION 2. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-3201. Part definitions.

As used in this part:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. As used in this subdivision (1), "control" or "controlled" means:

(A) Ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of a class of voting security of a company;

(B) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) The power to exercise controlling influence over the management of a company;

(2) "Authenticate" means to verify using reasonable means that a consumer who is entitled to exercise the rights in § 47-18-3203, is the same

consumer who is exercising those consumer rights with respect to the personal information at issue;

(3) "Biometric data":

(A) Means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual; and

(B) Does not include a physical or digital photograph, video recording, or audio recording or data generated from a photograph or video or audio recording; or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA;

(4) "Business associate" has the same meaning as defined by HIPAA;

(5) "Child" means a natural person younger than thirteen (13) years of age;

(6) "Consent":

(A) Means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer; and

(B) Includes a written statement, including a statement written by electronic means, or an unambiguous affirmative action;

(7) "Consumer":

(A) Means a natural person who is a resident of this state acting only in a personal context; and

(B) Does not include a natural person acting in a commercial or employment context;

(8) "Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information;

(9) "Covered entity" has the same meaning as defined by HIPAA;

(10) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to basic necessities, such as food and water;

(11) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual;

(12) "Health record":

(A) Means a written, printed, or electronically recorded material that:

(i) Was created or is maintained by a healthcare entity described in or licensed under title 68 in the course of providing healthcare services to an individual; and

(ii) Concerns the individual and the services provided; and

(B) Includes the substance of a communication made by an individual to a healthcare entity described in or licensed under title 68 in confidence during or in connection with the provision of healthcare services or information otherwise acquired by the healthcare entity about an individual in confidence and in connection with the provision of healthcare services to the individual;

(13) "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.);

(14) "Identified or identifiable natural person," "natural person," and "individual" mean a human being who can be readily identified, whether directly or indirectly;

(15) "Institution of higher education" means a public or private institution of higher education;

(16) "Nonprofit organization" means:

(A) A corporation organized under the Tennessee Nonprofit Corporation Act, compiled in title 48, chapter 51;

(B) An organization exempt from taxation under the Internal Revenue Code, codified in 26 U.S.C. §§ 501-530;

(C) A public utility organized under the laws of this state; or

(D) An entity owned or controlled by a nonprofit organization;

(17) "Personal information":

(A) Means information that is linked or reasonably linkable to an identified or identifiable natural person; and

(B) Does not include information that is:

(i) Publicly available information; or

(ii) De-identified or aggregate consumer information;

(18) "Precise geolocation data":

(A) Means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750'); and

(B) Does not include:

(i) The content of communications; or

(ii) Data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

(19) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal information;

(20) "Processor" means a natural or legal entity that processes personal information on behalf of a controller;

(21) "Profiling" means a form of solely automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(22) "Protected health information" has the same meaning as defined by HIPAA;

(23) "Pseudonymous data" means personal information that cannot be attributed to a specific natural person without the use of additional information, so long as the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable natural person;

(24) "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(25) "Sale of personal information":

(A) Means the exchange of personal information for valuable monetary consideration by the controller to a third party; and

(B) Does not include:

(i) The disclosure of personal information to a processor that processes the personal information on behalf of the controller;

(ii) The disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer;

(iii) The disclosure or transfer of personal information to an affiliate of the controller;

(iv) The disclosure of information that the consumer:

(a) Intentionally made available to the general public via a channel of mass media; and

(b) Did not restrict to a specific audience; or

(v) The disclosure or transfer of personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

(26) "Sensitive data" means a category of personal information that includes:

(A) Personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

(B) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

(C) The personal information collected from a known child; or

(D) Precise geolocation data;

(27) "State agency" means an agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch;

(28) "Targeted advertising":

(A) Means displaying to a consumer an advertisement that is selected based on personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests; and

(B) Does not include:

(i) Advertisements based on activities within a controller's own websites or online applications;

(ii) Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(iii) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) Personal information processed solely for measuring or reporting advertising performance, reach, or frequency;

(29) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller; and

(30) "Trade secret" means information, without regard to form, including, but not limited to, technical, nontechnical, or financial data, a formula, pattern, compilation, program, device, method, technique, plan, or process, that:

(A) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(B) Is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

47-18-3202. Scope.

This part applies to persons that conduct business in this state producing products or services that target residents of this state and that:

(1) Exceed twenty-five million dollars ($25,000,000) in revenue; and

(2)

(A) Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information; or

(B) During a calendar year, control or process personal information of at least one hundred thousand (100,000) consumers.

47-18-3203. Personal information rights – Consumers.

(a)

(1) A consumer may invoke the consumer rights authorized pursuant to subdivision (a)(2) at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights authorized pursuant to subdivision (a)(2) on behalf of the child regarding processing personal information belonging to the known child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(A) Confirm whether a controller is processing the consumer's personal information and to access the personal information;

(B) Correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer's personal information;

(C) Delete personal information provided by or obtained about the consumer. A controller is not required to delete information that it maintains or uses as aggregate or de-identified data; provided, that such data in the possession of the controller is not linked to a specific consumer. A controller that obtained personal information about a consumer from a source other than the consumer is in compliance with a consumer's request to delete such personal information by:

(i)

(a) Retaining a record of the deletion request and the minimum information necessary for the purpose of ensuring that the consumer's personal information remains deleted from the controller's records; and

(b) Not using such retained personal information for any purpose prohibited under this part; or

(ii) Opting the consumer out of the processing of such personal data for any purpose except for those exempted under this part;

(D) Obtain a copy of the consumer's personal information that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; or

(E) Opt out of a controller's processing of personal information for purposes of:

(i) Selling personal information about the consumer;

(ii) Targeted advertising; or

(iii) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) Except as otherwise provided in this part, a controller shall comply with an authenticated request by a consumer to exercise the consumer rights authorized pursuant to subdivision (a)(2) as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of a request submitted pursuant to subsection (a). The response period may be extended once by forty-five (45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension;

(2) If a controller declines to take action regarding the consumer's request, then the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection (c);

(3) Information provided in response to a consumer request must be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, technically infeasible, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or repetitive nature of the request; and

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller is not required to comply with

a request to initiate an action under subsection (a) and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision (b)(2). The appeal process must be made available to the consumer in a conspicuous manner, must be available at no cost to the consumer, and must be similar to the process for submitting requests to initiate action pursuant to subsection (a). Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, then the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general and reporter to submit a complaint.

47-18-3204. Data controller responsibilities – Transparency.

(a) A controller shall:

(1) Limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;

(2) Except as otherwise provided in this part, not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which the personal information is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices, as described in § 47-18-3213, to protect the confidentiality, integrity, and accessibility of personal information. The

data security practices must be appropriate to the volume and nature of the personal information at issue;

(4) Not be required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;

(5) Not process personal information in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising the consumer rights contained in this part, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, this subdivision (a)(5) does not require a controller to provide a product or service that requires the personal information of a consumer that the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to § 47-18-3203(a)(2)(F) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

(6) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and its implementing regulations.

(b) A provision of a contract or agreement that purports to waive or limit the consumer rights described in § 47-18-3203 is contrary to public policy and is void and unenforceable.

(c) A controller shall provide a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) The categories of personal information processed by the controller;

(2) The purpose for processing personal information;

(3) How consumers may exercise their consumer rights pursuant to § 47-18-3203, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) The categories of personal information that the controller sells to third parties, if any; and

(5) The categories of third parties, if any, to whom the controller sells personal information.

(d) If a controller sells personal information to third parties or processes personal information for targeted advertising, then the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(e)

(1) A controller shall provide, and shall describe in a privacy notice, one (1) or more secure and reliable means for a consumer to submit a request to exercise the consumer rights in § 47-18-3203. Such means must take into account the:

(A) Ways in which a consumer normally interacts with the controller;

(B) Need for secure and reliable communication of such requests; and

(C) Ability of a controller to authenticate the identity of the consumer making the request.

(2) A controller shall not require a consumer to create a new account in order to exercise consumer rights in § 47-18-3203, but may require a consumer to use an existing account.

47-18-3205. Responsibility according to role – Controller and processor.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this part. The assistance must include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 47-18-3203; and

(2) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 47-18-3206.

(b) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor shall:

(1) Ensure that each person processing personal information is subject to a duty of confidentiality with respect to the data;

(2) At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law;

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this part;

(4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and

(5) Engage a subcontractor pursuant to a written contract in that requires the subcontractor to meet the obligations of the processor with respect to the personal information.

(c) This section does not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as described in subsection (b).

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

47-18-3206. Data protection assessments.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal information:

(1) The processing of personal information for purposes of targeted advertising;

(2) The sale of personal information;

(3) The processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Processing activities involving personal information that present a heightened risk of harm to consumers.

(b) Data protection assessments conducted pursuant to subsection (a) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal information will be processed, must be factored into this assessment by the controller.

(c) The attorney general and reporter may request pursuant to a civil investigative demand that a controller disclose a data protection assessment that is relevant to an investigation conducted by the attorney general and reporter, and the controller shall make the data protection assessment available to the attorney general and reporter. The attorney general and reporter may evaluate the data protection assessment for compliance with the responsibilities set forth in § 47-18-3204. Data protection assessments are confidential and not open to public inspection and copying. The disclosure of a data protection assessment pursuant to a request from the attorney

general and reporter does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and information contained in the assessment.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) Data protection assessments conducted by a controller for the purpose of compliance with other laws, rules, or regulations may comply with this section if the assessments have a reasonably comparable scope and effect.

(f) Data protection assessment requirements apply to processing activities created or generated on or after July 1, 2024, and are not retroactive.

47-18-3207. Processing de-identified data – Exemptions.

(a) The controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with a natural person;

(2) Publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and

(3) Contractually obligate recipients of the de-identified data to comply with this part.

(b) This section does not require a controller or processor to:

(1) Reidentify de-identified data or pseudonymous data;

(2) Maintain data in identifiable form, or collect, obtain, retain, or access data or technology, in order to be capable of associating an authenticated consumer request with personal information; or

(3) Comply with an authenticated consumer rights request, pursuant to § 47-18-3203, if:

(A) The controller is not reasonably capable of associating the request with the personal information or it would be unreasonably

burdensome for the controller to associate the request with the personal information;

(B) The controller does not use the personal information to recognize or respond to the specific consumer who is the subject of the personal information, or associate the personal information with other personal information about the same specific consumer; and

(C) The controller does not sell the personal information to a third party or otherwise voluntarily disclose the personal information to a third party other than a processor, except as otherwise permitted in this section.

(c) The consumer rights contained in §§ 47-18-3203 and 47-18-3204 do not apply to pseudonymous data in cases where the controller is able to demonstrate information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing that information.

(d) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.

47-18-3208. Limitations.

(a) This part does not restrict a controller's or processor's ability to:

(1) Comply with federal, state, or local laws, rules, or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(4) Investigate, establish, exercise, prepare for, or defend legal claims;

(5) Provide a product or service specifically requested by a consumer or the parent or legal guardian of a known child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;

(8) Engage in public- or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entity that determines whether:

(A) Deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) The expected benefits of the research outweigh the privacy risks; and

(C) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification; or

(9) Assist another controller, processor, or third party with the obligations under this part.

(b) The obligations imposed on controllers or processors under this part do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) Conduct internal research to develop, improve, or repair products, services, or technology;

(2) Effectuate a product recall;

(3) Identify and repair technical errors that impair existing or intended functionality; or

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under this part do not apply where compliance by the controller or processor with this part would violate an evidentiary privilege under the laws of this state. This part does not prevent a controller or processor from providing personal information concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(d)

(1) A controller or processor that discloses personal information to a third-party controller or processor, in compliance with the requirements of this part, is not in violation of this part if:

(A) The third-party controller or processor that receives and processes the personal information is in violation of this part; and

(B) At the time of disclosing the personal information, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal information from a controller or processor in compliance with the requirements of this part is likewise not in violation of this part for the violations of the controller or processor from which it receives such personal information.

(e) This part does not impose an obligation on controllers and processors that adversely affects the rights or freedoms of a person, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal information by a person in the course of a purely personal activity.

(f) A controller shall not process personal information for purposes other than those expressly listed in this section unless otherwise allowed by this part. Personal information processed by a controller pursuant to this section may be processed to the extent that the processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section; and

(2) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal information collected, used, or retained pursuant to subsection (b) shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention. The data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal information and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal information.

(g) If a controller processes personal information pursuant to an exemption in this section, then the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with subsection (f).

(h) Processing personal information for the purposes expressly identified in subdivisions (a)(1)-(9) does not solely make an entity a controller with respect to the processing.

47-18-3209. Investigative authority.

If the attorney general and reporter has reasonable cause to believe that an individual, controller, or processor has engaged in, is engaging in, or is about to engage in a violation of this part, then the attorney general and reporter may issue a civil investigative demand.

47-18-3210. Exemptions.

(a) This part does not apply to:

(1) A body, authority, board, bureau, commission, district, or agency of this state or of a political subdivision of this state;

(2) A financial institution, an affiliate of a financial institution, or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);

(3) An individual, firm, association, corporation, or other entity that is licensed in this state under title 56 as an insurance company and transacts insurance business;

(4) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, 45 CFR Parts 160 and 164 established pursuant to HIPAA, and the federal Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

(5) A nonprofit organization;

(6) An institution of higher education;

(7) Protected health information under HIPAA;

(8) Health records for purposes of title 68;

(9) Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

(10) Personal information:

(A) Processed for purposes of:

(i) Research conducted in accordance with the federal policy for the protection of human subjects under 45 CFR Part 46;

(ii) Human subjects research conducted in accordance with good clinical practice guidelines issued by The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; or

(iii) Research conducted in accordance with the protection of human subjects under 21 CFR Parts 6, 50, and 56; or

(B) Processed or sold in connection with research conducted in accordance with the requirements set forth in this part, or other research conducted in accordance with applicable law;

(11) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

(12) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

(13) Information that is:

(A) Derived from the healthcare-related information listed in this subsection (a) that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; or

(B) Included in a limited data set as described in 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified in 45 CFR 164.514(e);

(14) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under

this subsection (a) that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

(15) Information used only for public health activities and purposes as authorized by HIPAA;

(16) The collection, maintenance, disclosure, sale, communication, or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(17) Personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

(18) Personal information or educational information regulated by the federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g et seq.);

(19) Personal information collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.);

(20) Data processed or maintained:

(A) In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(B) As the emergency contact information of an individual under this part used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the individual under subdivision (a)(20)(A) and used for the purposes of administering those benefits;

(21) Information collected as part of public- or peer-reviewed scientific or statistical research in the public interest; or

(22) An insurance producer licensed under title 56.

(b) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) are deemed compliant with an obligation to obtain parental consent under this part.

(c) This part does not require a controller, processor, third party, or consumer to disclose trade secrets.

47-18-3211. Contracts.

(a) A provision of a contract or agreement that waives or limits a consumer's rights under this part, including, but not limited to, a right to a remedy or means of enforcement, is contrary to public policy, void, and unenforceable.

(b) This part does not prevent a consumer from declining to request information from a controller, declining to opt out of a controller's sale of the consumer's personal information, or authorizing a controller to sell the consumer's personal information after previously opting out.

(c) This part applies to contracts entered into, amended, or renewed on or after the effective date of this act.

47-18-3212. Enforcement – Civil penalty – Expenses.

(a) The attorney general and reporter has exclusive authority to enforce this part.

(b) The attorney general and reporter may develop reasonable cause to believe that a controller or processor is in violation of this part, based on the attorney general and reporter's own inquiry or on consumer or public complaints. Prior to initiating an action under this part, the attorney general and reporter shall provide a controller or

processor sixty-days' written notice identifying the specific provisions of this part the attorney general and reporter alleges have been or are being violated. If within the sixty-day period, the controller or processor cures the noticed violation and provides the attorney general and reporter an express written statement that the alleged violations have been cured and that no such further violations shall occur, then the attorney general and reporter shall not initiate an action against the controller or processor.

(c) If a controller or processor continues to violate this part following the cure period in subsection (b) or breaches an express written statement provided to the attorney general and reporter under subsection (b), then the attorney general and reporter may bring an action in a court of competent jurisdiction seeking any of the following relief:

(1) Declaratory judgment that the act or practice violates this chapter;

(2) Injunctive relief, including preliminary and permanent injunctions, to prevent an additional violation of and compel compliance with this part;

(3) Civil penalties, as described in subsection (d);

(4) Reasonable attorney's fees and investigative costs; or

(5) Other relief the court determines appropriate.

(d)

(1) A court may impose a civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation of this part.

(2) If the court finds the controller or processor willfully or knowingly violated this part, then the court may, in its discretion, award treble damages.

(e) A violation of this part shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this part or other law.

(f) The attorney general and reporter may recover reasonable expenses incurred in investigating and preparing a case, including attorney fees, in an action initiated under this part.

47-18-3213. Affirmative defense – Voluntary privacy program.

(a) A controller or processor has an affirmative defense to a cause of action for a violation of this part if the controller or processor creates, maintains, and complies with a written privacy policy that:

(1)

(A) Reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0." or another comparable privacy framework; and

(B) Is updated to reasonably conform with a subsequent revision to the NIST or comparable privacy framework within two (2) years of the publication date stated in the most recent revision to the NIST or comparable privacy framework; and

(2) Provides a person with the substantive rights required by this part.

(b) The scale and scope of a controller or processor's privacy program under subsection (a) is appropriate if it is based on all of the following factors:

(1) The size and complexity of the controller or processor's business;

(2) The nature and scope of the activities of the controller or processor;

(3) The sensitivity of the personal information processed;

(4) The cost and availability of tools to improve privacy protections and data governance; and

(5) Compliance with a comparable state or federal law.

(c)

(1) In addition to subsections (a) and (b):

(A) A controller may be certified pursuant to the Asia Pacific Economic Cooperation's Cross Border Privacy Rules system; and

(B) A processor may be certified pursuant to the Asia Pacific Economic Cooperation's Privacy Recognition for Processors system.

(2) Certifications under subdivision (c)(1) may be considered in addition to the factors in subsection (b).

SECTION 3. If a provision of this act or its application to a person or circumstance is held invalid, then the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to that end, the provisions of this act are severable.

SECTION 4. This act supersedes and preempts any conflicting provisions of any public or private act and laws, ordinances, resolutions, regulations, or the equivalent adopted by a home rule municipality, county, including a metropolitan government, or city regarding the processing of personal data by controllers or processors. To the extent there exists a conflict, this section does not require the home rule municipality, county, or city to adopt any law, ordinance, resolution, regulation, or the equivalent to modify or repeal such conflicting provisions enacted prior to the effective date of this act.

SECTION 5. The headings in this act are for reference purposes only and do not constitute a part of the law enacted by this act. However, the Tennessee Code Commission is requested to include the headings in any compilation or publication containing this act.

SECTION 6. This act takes effect July 1, 2025, the public welfare requiring it.